CLAIM AMENDMENTS

The following is a complete listing of the pending claims:

Claims 1 – 19. (cancelled)

20. (Previously Presented) A storage device, comprising:

a storage medium; and

a storage engine, the storage engine being configured to generate a secure session key and to receive encrypted content and a corresponding encrypted content key from a host system, wherein the content key has been encrypted by the host system using the secure session key, the storage engine being further configured to decrypt the encrypted content key using the secure session key and to encrypt the decrypted content key with a first storage engine encryption key and to write the storage-engine-encrypted content key to the storage medium.

21. (Previously Presented) The storage device of claim 20, wherein the storage engine is further configured to generate the secure session key in response to verifying the authenticity of a certifying authority's digital signature provided by the host system.

22. (Previously Presented) The storage device of claim 21, wherein the storage engine is further configured to encrypt the secure session key using a public key provided by the host system such that the host system can recover the secure

session key only by decrypting the encrypted secure session key using the private key corresponding to the public key.

23. (Previously Presented) The storage device of claim 22, wherein the storage engine is further configured to doubly-encrypt the encrypted content using at least a second storage engine encryption key.

24. (Previously Presented) The storage device of claim 23, wherein the second storage engine encryption key comprises a Data Encryption Standard (DES) key.

25. (Previously Presented) The storage device of claim 24, wherein the DES key comprises a triple DES key.

26. (cancelled)

27. (currently amended) The storage device of claim 25 ~~26~~, wherein the optical disc is a removable optical disc.

28. (Previously Presented) The storage device of claim 22, wherein the public key and the private key are elliptic curve cryptography keys.

29. (Previously Presented) The storage device of claim 20, wherein the storage engine includes a random number generator for generating the secure session key.

30. (Previously Presented) A method of writing to a storage device from a host system having a public key and a corresponding private key, comprising:

encrypting a secure session key using the public key;

recovering the secure session key from the encrypted secure session key using the corresponding private key;

encrypting content according to a content key and commanding the storage device to write the encrypted content to a storage medium;

encrypting the content key using the secure session key and transmitting the encrypted content key to the storage device; and

in the storage device, decrypting the encrypted content key using the secure session key.

31. (cancelled).